Chapter 17
Human Factor Role for Cyber Threats Resilience

Zlatogor Borisov Minchev
Institute of ICT, Bulgarian Academy of Sciences, Bulgaria

ABSTRACT

The chapter describes the problem of building cyber threats resilience for the human factor as the technological growth is constantly changing the security landscape of the new digital world. A methodological framework for meeting the problem by using the "scenario method" and experts' support is outlined. An implementation of comprehensive morphological and system analyses of cyber threats are performed, followed by agent based mixed reality validation, incorporating biometrics monitoring. The obtained results demonstrate a correlation of experts' beliefs for cyber threats identification, related to human factor biometric response, whilst using social networks and inhabiting smart environments of living. The achieved results prove "use with care" necessity for new technologies, concerning cyber threats landscape for assuring a sustainable resilience balance from the human factor perspective.

INTRODUCTION

Today digital technologies are inevitably changing our way of living and social organization in general. These yield the relevant transformations towards digital society progress, forecasted by Toffler in the broader informational context, over thirty years ago (Toffler, 1981).

The process obviously constitutes rather slowly in comparison with the technological growth, but quite sustainable in its social profile, together with the understanding and future digital culture change.

We are already living in a world that requires engagement, autonomy and agility from both technologies and people with their relevant organization and environment of growth.

The last could be generalized around the "resilience", or a multiaspect aftermath disasters/attacks sustainable recovering capabilities development (Cho, Willis, & Stewart-Weeks, 2011).

Generally, the "resilience" idea is also believed to be related to psychology (Hind, Frost & Rowley, 1996; Ruttner, 1990; Windle, 2011), management (Sheffi, 2005) and even social systems (Holling & Gunderson, 2002), addressing their "robustness" (Beinhocker, 1999; Deevy, 1995) towards multiple influences.

In practice, to cope the idea in general is related with discovering a fitting mechanism for the

DOI: 10.4018/978-1-4666-8793-6.ch017

world towards people – human factors, taking into account the existence and prevention of multiple threats enablers and resulting risks for producing a better society.

Several good studies for social changes resilience exploration to mark: SECRES public study ("SECRES Project Report", 2008) that is encompassing a ten-year endeavor in the field; EU and the Greater Black Sea Area FOCUS ("FOCUS Project Web Page", 2011), CRISHOPE (Ionescu, 2012) and DRIVER ("DRIVER Project Web Page", 2014) initiatives.

These however mostly address the social side of the resilience, noting the importance of crisis management for different manmade and natural disasters from the comprehensive security perspective.

When talking about the cyber aspect of the resilience nowadays, a close connection to the Internet technologies progress, influence and expected threats have to be discussed.

Meeting the problem from the cyber space perspective was recently organized around FORWARD project efforts ("FORWARD Project Web Page", 2007) and its follower – EU Network of Excellence SysSec ("SysSec Project Web Page", 2010), outlining future cyber space threats in a global scale and trying to be proactive.

In the present technological context, this directly encompasses social networks, together with smart cities, homes, cloud services and "Internet Of Things", facing multiple sensors and gadgets, that current organization is expected to become more intelligent and integrated in the future Web 4.0 (Boyanov, 2014; Höller et al., 2014).

Other studies of different aspects of the cyber threats landscape evolution are focusing social networks and human factor response ("DMU 03/22 Project Web Page", 2012), future smart homes cyber threats identification ("DFNI T01/4 Project Web Page", 2012) and also giving a special attention to the human factor biometrics dynamics monitoring and analysis during multiple sensory conflicts ("TK 02/60 Project Web Page", 2010).

What however has to be noted again here is the key position of the human factor response. Being in general a source of technological innovations and, at the same time, affected from the new disruptive devices and services penetration in the digital daily life, the human factor has a key role for establishing resilience.

And going deeper into the problem of fitting mechanism building, the different cyber risks and threats landscape has to be studied from multiple projections and situational significance dynamics.

This process could not just be performed in general. Usually the system of exploration is large and complex enough, thus quite unstable (Ashby, 2012) and difficult for maintenance and forecasting.

Concerning the exploration of technological-human fitting, two other key points deserve attention as well:

1. Being proactive, and
2. Developing agility.

The proactive approach, closely related towards meeting complicated and unexpected attacks with multiple external influences (e.g.: crisis events, advanced persistent threats, innovative exploits, social engineering, etc.), saving desired services, systems functionalities, and allowing, at the same time, a technological progress growing, together with human factor relevant attitude towards all these dynamic changes.

In regards to this attitude, a technological and human perspective should also be noticed.

The different cyber threats nature can easily be divided into: outside and inside area, describing the system of interest. Whilst, the outside threats are easy to be understand as motivation and objectives, the inside ones are much more difficult to be discovered and forecasted.

Apart of this, the fast technological progress is producing intelligent devices that can evolve in the wrong direction for their users and produce